RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAW-W08

Risk Whisperers: Decoding Cyber Insurance

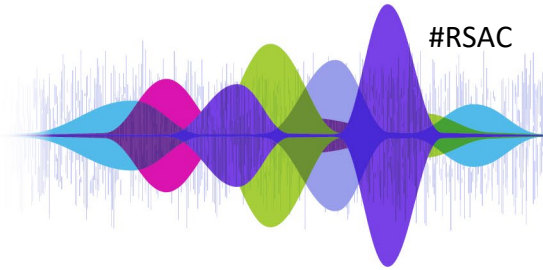
MODERATOR: **Christopher Seusing**
Partner, Wood, Smith Henning & Berman LLP
https://www.linkedin.com/in/chrisseusing/

PANELISTS: **Violet Sullivan**
AVP, Cyber Services
Crum & Forster
https://www.linkedin.com/in/txcyberlawyer/

Peter Hedberg
VP, Cyber Underwriting
Corvus Insurance (Travelers)
https://www.linkedin.com/in/peterhedberg/

Monique Ferraro
Cyber Counsel
HSB (Munich Re)
https://www.linkedin.com/in/monique-ferraro-bb47167/

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:

Christopher Seusing

Wood, Smith, Henning & Berman
https://www.linkedin.com/in/chrisseusing/

PANELISTS:

Violet Sullivan

Crum & Forster
https://www.linkedin.com/in/txcyberlawyer/

Peter Hedberg

Corvus Insurance
https://www.linkedin.com/in/peterhedberg/

Monique Ferraro

HSB
https://www.linkedin.com/in/monique-ferraro-bb47167/

Agenda

Very brief overview of cyber insurance and current challenges

What we're seeing in claims

Emerging and future issues

RSAC 2025 Conference

Coverages and Types of Policies

Types of policies

- Standalone
- Package/endorsements
  - Commercial Property Package
  - Business Owners Policy
  - Errors & Omissions
  - Professional liability
  - Directors & Officers
  - Homeowners
  - Auto

Typical coverages

- Cyber attacks
- Data breach (usually via computer or hard copy)
- Wire transfer fraud and fraudulent funds transfer
- Media liability
- Business interruption/contingent business interruption
- Privacy law inadvertent violations
- Fines & penalties (where allowed)
- Payment Card Industry
- System failure
- Specific generative artificial intelligence in some policies

Catastrophe Bonds

- Insurance linked securities
  - To cover cyber catastrophe
  - Very new, lots of wrinkles
    - Crowdstrike first challenge, didn’t cover outages/dependencies

RSAC™ 2025 Conference

Apply

Many Voices.
One Community.

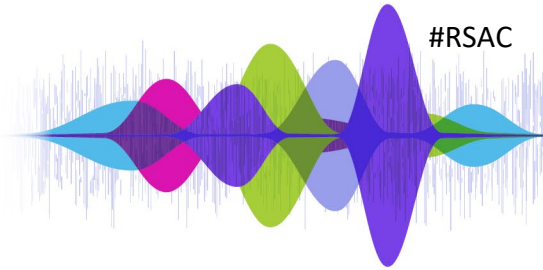
Apply What You Have Learned Today

- Next week you should:
  - Reach out to your risk manager or insurer to learn about your cyber insurance policy
  - Identify approved remediation/restoration vendors you feel comfortable working with
  - If you do not have cyber insurance yet, it's time
    - Contact the risk manager and if you don't have a risk manager, reach out to your broker
- In the first three months following this presentation you should:
  - Meet with your broker and review recommended policies if you don't already have cyber insurance
    - Apply for a cyber insurance policy
- Within six months you should:
  - Review broker recommendations for next year's renewal and investigate whether implementation is feasible

RSAC 2025 Conference

Current Trends and Challenges to Existing Coverages

Cyber insurance market 2025



- Munich Re predicts $16B in premium
- Woodruff Sawyer, brokers, predict increased cyber risks and increased premiums despite soft market
- Gallagher- market is stabilizing with competitive rates, lots of capacity and increased availability of discounted, complimentary or embedded services

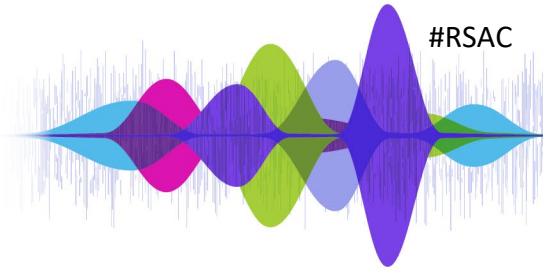
Coverage Trends

- More carriers offering cybersecurity tools directly, such as endpoint monitoring
- Coverage for chief information security officer liability can be found in cyber, Directors & Officers, Errors & Omissions or stand alone policies.
- More focus on third party risks

The AI Challenge

- Facilitates phishing
  - More sophisticated and more accurate emails/messaging
  - Can get more done more efficiently- higher frequency of attacks
- Makes malware generation easier
  - Easier to modify existing malware to make it fit for purpose, evade antivirus
- Unintentional copyright infringement
  - Large Language Models trained on copyrighted material, unintentional copyright infringement still infringement
  - Media liability impact- has not hit yet, but we are concerned
- Deepfakes
  - Facilitates wire transfer fraud, business email compromise, social engineering

What will insurers do about generative artificial intelligence?



- Possible exclusions- Insurance Services Office has developed exclusions
- Possible affirmative coverages
- Puzzling over “silent” risks in other types of policies
- Tighter underwriting that considers use of generative artificial intelligence and governance
- Require certain controls, such as in-person confirmations of client information changes, accounts payable information

RSAC™ 2025 Conference

Apply

Many Voices.
One Community.

Apply What You Have Learned Today

- Next week you should:
  - Review your cyber policy to see what complimentary/discounted services come along with your policy
  - Identify insurer approved vendors on pre-incident and claims panels
  - Identify approved vendors you feel comfortable working with
  - Review privacy and artificial intelligence use and internal policies
- In the first three months following this presentation you should:
  - Meet vendors on your cyber insurer's panel
  - Review compliance with privacy and artificial intelligence laws/regulations
- Within six months you should:
  - Implement security, privacy controls and implement tweaks & risk mitigation
  - Set up regular (once a year is fine) meetings with your response vendors

RSAC 2025 Conference

Claims Activity

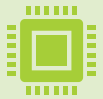
Severity of cyber attacks

$10.5 trillion estimated in 2025, according to Cybercrime Magazine

$5.24 million per malware attack (UpGuard)

According to Sophos, ransom payments up 500% from 2023 to 2024, with average payment of $2 million

Severity (cost) of claims and how to mitigate



According to IBM, the average cost of a data breach rose 10% from 2023 to 2024 to $4.88 million globally, $9.36 million for US businesses

Healthcare, finance, pharmaceuticals, tech, energy, and professional services are the most at-risk

The cost of a ransom varies based on the industry and size of the business, and it typically ranges from 1%-5% of annual revenue

Other data breach costs- loss of business due to reputation damage, higher customer conversion costs, lost market share, and stock price movement

Higher Frequency and Severity

- Generative artificial intelligence facilitating phishing
  - Fewer grammatical errors
  - Targeting more focused and customized
  - Makes business email compromise more efficient
  - Customized ransomware and extortion attacks
- Wire transfer fraud and fraudulent funds transfer
  - More attempts
  - Higher amounts
- Deepfake hires getting foothold in system to surveille & compromise
  - Law enforcement very concerned, at least 300 business affected in past few months
  - Escalate permissions
  - Nation state connections
- Privacy litigation
  - Tracking litigation

Costs of an attack or data breach can be SUBSTANTIALLY reduced (reportedly 40% or more) by implementing

- Adequate, tested, air-gapped backups
- AI and automation into cyber security program (endpoint monitoring, etc.)
- Knowing WHAT data one has and putting controls around it (encryption, MFA, biometrics)
- Awareness training
- Incident response plan (practice, practice practice!)

RSAC™ 2025 Conference

Apply

Many Voices.
One Community.

Apply What You Have Learned Today

- Next week you should:
  - Review your exposure to enhanced and more sophisticated phishing
  - Review backup processes
  - Review control processes around accounts payable changes in addresses, bank account information and limit approvals
- In the first three months following this presentation you should:
  - Draft plans to remediate any deficiencies identified the first week
- Within six months you should:
  - Implement plans to remediate deficiencies

RSAC 2025 Conference

Emerging and Future Issues

Emerging Issues

- State privacy laws
  - 20 states have comprehensive laws
  - Not just data breach
  - Wrongful collection
  - Some have right of private lawsuits
- New laws will increase demand for more sophisticated legal representation and will increase the length of time from claim to resolution
- Privacy coverage for first and third party claims will be tested

Emerging issues

- State artificial intelligence laws
  - Differing requirements make compliance more challenging
  - We are waiting to see what impact there will be- so far hard to tell, but we know it's there
  - As with privacy laws, the more there are, and the more differences, the greater the need for sophisticated legal counsel and remediation services
- Coverages within cyber policies likely will cover inadvertent violations, investigation costs, remediation
- This will be a source of confusion for a while, just as privacy was. Different insurers and policies will have different language, so using a knowledgeable broker is essential

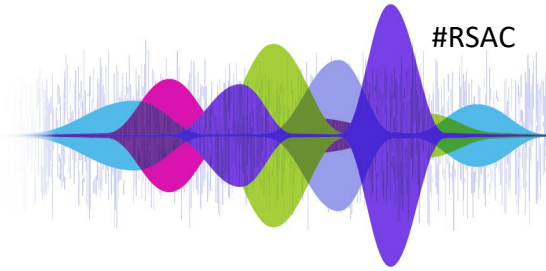
Emerging issues

- Catastrophe planning
  - Working groups with feds and insurers collaborating on planning for economic support have paused
  - We have not yet seen a “cyber catastrophe,” so it is largely unknown what will qualify, whether it will ever happen and if there is sufficient capacity in insurance to cover it when/if it happens
  - Unknown to what extent new “widespread event” coverage and exemptions will be effective in the event of a cyber catastrophe

Emerging issues

- Federal regulatory enforcement
  - Layoffs and agency closers likely to result in fewer federal actions by Federal Trade Commission and the Department of Health and Human Services Office of Civil Rights will likely result in fewer federal enforcement actions
  - States will likely step in, making enforcement less predictable and inconsistent
  - Uncertainty may lead to higher premiums and tighter underwriting
- Layoffs within Cybersecurity and Infrastructure Security Agency, Cyber Command and other federal cyber agencies
  - Likely to attract more frequent, more severe attacks
  - Trade and other conflicts may fuel nation state attacks, which in turn may invoke the “cyber war exclusions” which have not yet been tested

And finally. . .



- Proliferation of generative artificial intelligence and agentic artificial intelligence
  - Increase the potential for automated attacks, making claims under cyber policies more frequent and more severe
  - Agentic malware and attacks may be more persistent and difficult to stop and remediate
  - This will likely challenge cyber policy limits of coverage

RSAC™ 2025 Conference

Apply

Many Voices.
One Community.

Apply What You Have Learned Today

- Next week you should:
  - Investigate your compliance with state privacy and generative artificial intelligence laws
  - Does your company have a generative artificial intelligence policy?
  - How about governance? What does your company have in place and what are they planning to set up?
  - Take a look at your incident response and disaster recovery plans to see if they would address a cyber catastrophe
- In the first three months following this presentation you should:
  - Create a plan to address deficiencies you may find in your compliance regime and/or reach out to stakeholders to collaborate if that is not taking place already
- Within six months you should:
  - Test any additions and revisions to your incident and disaster recovery plans

RSAC 2025 Conference

Q & A

Don’t hold back. Hit us with your toughest questions

Many Voices.
One Community.

RSAC 2025 Conference

Many Voices.
One Community.

Contact us on LinkedIn or email:

cseusing@wshblaw.com

violet.sullivan@cfins.com

phedber3@corvusinsurance.com

monique_ferraro@hsb.com